

Agreement on the processing of personal data

Between the

Customer

as client

- hereinafter referred to as the client -

and

Planubo, Christoph Drechsler & Michael Tenzer GbR

Am Hirtengarten 2

77743 Neuried

as contractor

- hereinafter referred to as Contractor -

1 Introduction, scope of application, definitions

- (1) This contract regulates the rights and obligations of the client and contractor (hereinafter referred to as the "parties") in the context of processing personal data on behalf of the client.
- (2) Terms used in this contract are to be understood in accordance with their definition in the EU General Data Protection Regulation. In this sense, the client is the "controller" and the contractor is the "processor". Insofar as declarations are to be made "in writing" in the following, the written form pursuant to Section 126 BGB is meant. Otherwise, declarations may also be made in another form, provided that appropriate verifiability is guaranteed.

2 Object and duration of processing

2.1 Object

The subject matter of the agreement is the rights and obligations of the parties in the context of the provision of services in accordance with the order, the service description and the GTC (hereinafter referred to as the main contract), insofar as personal data is processed by the contractor as a processor for the client in accordance with Art. 28 GDPR. This includes all activities that the contractor carries out to fulfill the order and that constitute order processing. This also applies if the order does not expressly refer to this agreement on order processing.

2.2 Duration

Processing shall commence on the start date agreed in the order and shall continue indefinitely until this contract or the main contract is terminated by one of the parties.

3 Type, purpose and data subjects of the data processing:

3.1 Nature and purpose of processing

The Contractor shall provide the services for the Client in accordance with the main contract. In addition, it shall provide maintenance and support services for the Client, as a result of which there is the possibility of access to the types of personal data listed below, which are processed with the software or stored on the storage space provided.

3.2 Type of data

The following data is processed:

- The type of data processed is determined by the client through the configuration and use of the services. The data to be processed may include first and last name, e-mail address, IP address, address, event data, billing data and profile settings.

3.3 Categories of data subjects

The following are affected by the processing:

- The categories of data subjects are determined by the client through the configuration and use of the services. The data subjects may include customers of the client, interested parties of the client and employees of the client.

4 Obligations of the contractor

- (1) The Contractor shall process personal data exclusively as contractually agreed, unless the Contractor is legally obliged to carry out specific processing. If such obligations exist for the contractor, the

contractor shall inform the client of these prior to processing, unless the notification is prohibited by law.

- (2) The Contractor confirms that it is aware of the relevant general data protection regulations. He observes the principles of proper data processing.
- (3) The Contractor undertakes to maintain strict confidentiality during processing.
- (4) Persons who may obtain knowledge of the data processed in the order must undertake in writing to maintain confidentiality, unless they are already subject to a relevant confidentiality obligation by law.
- (5) The Contractor warrants that the persons employed by it for processing have been familiarized with the relevant provisions of data protection and this contract before the start of processing. Appropriate training and awareness-raising measures shall be repeated at regular intervals. The Contractor shall ensure that persons deployed for commissioned processing are appropriately instructed and monitored on an ongoing basis with regard to compliance with data protection requirements.
- (6) In connection with the commissioned processing, the Contractor shall support the Client to the extent necessary in fulfilling its obligations under data protection law, in particular in drawing up and updating the list of processing activities, in carrying out the data protection impact assessment and in consulting the supervisory authority if necessary. The required information and documentation shall be kept available and forwarded to the client on request. The Contractor shall be entitled to demand reasonable remuneration from the Client for these services.
- (7) If the Client is subject to an inspection by supervisory authorities or other bodies or if data subjects assert rights against it, the Contractor undertakes to support the Client to the extent necessary, insofar as the processing in the order is affected. The Contractor shall be entitled to demand reasonable remuneration from the Client for these services.
- (8) The Contractor may only provide information to third parties or the data subject with the prior consent of the Client. The Contractor shall forward any requests addressed directly to it to the Client without delay.
- (9) Where required by law, the contractor shall appoint a competent and reliable person as data protection officer. The contact details of the data protection officer are published on the contractor's website.

5 Safety of processing

- (1) The Contractor shall take appropriate technical and organizational measures in its area of responsibility to ensure that the processing is carried out in accordance with the requirements of the GDPR and guarantees the protection of the rights and freedoms of the data subject. The client shall take appropriate technical and organizational measures within its area of responsibility in accordance with Article 32 GDPR to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing on a permanent basis.
- (2) The Contractor's current technical and organizational measures can be viewed in Annex 1. These are descriptions of a technical nature which are to be regarded as part of this agreement.
- (3) The data security measures can be adapted in line with technical and organizational developments as long as they do not fall below the level of protection agreed here.

6 Regulations on the rectification, erasure and blocking of data

- (1) The Contractor shall only correct, delete or block data processed within the scope of the order in accordance with the contractual agreement made or in accordance with the Client's instructions.
- (2) If a data subject contacts the Contractor directly to exercise their data protection rights, the Contractor shall forward this request to the Client without delay.

7 Subcontracting relationships

- (1) The Client grants the Contractor general authorization to use further subcontractors within the meaning of Art. 28 GDPR for the performance of the contract.
- (2) The subcontractors currently used are listed in Annex 2. The client authorizes the use of these listed subcontractors. Outsourcing to further subcontractors and any change of existing subcontractors in accordance with Annex 2 are permitted, provided that:
 - a. the Contractor notifies the Client of such outsourcing or change in writing or in text form with a notice period of 4 weeks in advance and
 - b. the Client does not object to the planned outsourcing in writing or in text form to the Contractor within 2 weeks of receipt of the notification. In the event of an objection by the Client to such outsourcing or to the change of a subcontractor, the Contractor shall have the right to terminate this agreement and the main contract for good cause.
- (3) The rights of the client must also be able to be exercised effectively against the subcontractor.
- (4) The responsibilities of the contractor and the subcontractor must be clearly delineated.
- (5) The Contractor shall carefully select the subcontractor, paying particular attention to the suitability of the technical and organizational measures taken by the subcontractor.
- (6) If the Contractor awards contracts to other processors, the Contractor shall be responsible for transferring its data protection obligations under this Agreement to the other processor.
- (7) Subcontracting relationships within the meaning of this contract are only those services that are directly related to the provision of the main service. Ancillary services such as transportation, maintenance and cleaning as well as the use of telecommunications services or user services are not covered. The Contractor's obligation to ensure compliance with data protection and data security in these cases remains unaffected.

8 Rights and obligations of the client

- (1) The client alone is responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.
- (2) The client shall issue all orders, partial orders or instructions in writing. In urgent cases, instructions may be issued verbally. The client shall confirm such instructions in writing without delay.
- (3) The Client shall inform the Contractor immediately if it discovers errors or irregularities in the examination of the order results or irregularities with regard to data protection regulations.
- (4) In the event of termination, the client undertakes to delete the personal data stored in the services prior to the termination of the contract.
- (5) At the request of the Contractor, the Client shall appoint a contact person for data protection issues.

9 Inquiries from affected persons

- (1) If a data subject contacts the Contractor with a request for rectification, erasure or information, the Contractor shall refer the data subject to the Client, provided that the data subject can be assigned to the Client based on the information provided by the data subject. The Contractor shall forward the data subject's request to the Client without delay. The Contractor shall support the Client as far as possible. The Contractor shall not be liable if the Client fails to respond to the data subject's request, or fails to respond correctly or on time.

10 Instructions

- (1) Within the scope of this agreement, the Client is solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of the transfer of data to the Contractor and for the lawfulness of the data processing ("controller" within the meaning of Art. 4 No. 7 GDPR). This also applies with regard to the purposes and means of processing regulated in this agreement.
- (2) Instructions that are not provided for in the contract shall be treated as a request for a change in performance. In the event of proposed changes, the Contractor shall inform the Client of the effects on the agreed services. If the Contractor cannot reasonably be expected to carry out the instruction, the Contractor shall be entitled to terminate the processing.

11 Data processing outside the EU/EEA

- (1) As a rule, the contractually agreed data processing takes place predominantly in a member state of the European Union or in another state party to the Agreement on the European Economic Area. In the event that data is transferred to a third country, the contractor shall ensure that the requirements of Art. 44 et seq. GDPR are fulfilled.
- (2) The client authorizes the transfer of data to a third country to the recipients listed in Annex 2. The measures approved by the Client to ensure an adequate level of protection pursuant to Art. 44 et seq. GDPR in the context of subcontracting.
- (3) If the client instructs the transfer of data to third parties in a third country, the client shall be solely responsible for compliance with the provisions of Art. 44 et seq. GDPR is solely responsible.

12 Liability and compensation

- (1) In the event that a data subject asserts a claim for damages pursuant to Art. 82 GDPR, the parties undertake to support each other and to contribute to the clarification of the underlying facts.
- (2) The liability provision agreed between the parties in the main contract for the provision of services shall also apply to claims arising from this agreement on commissioned processing and in the internal relationship between the parties for claims of third parties pursuant to Art. 82 GDPR, unless expressly agreed otherwise.
- (3) The parties shall release each other from liability if/insofar as one party proves that it is in no way responsible for the circumstance that caused the damage to a person concerned.
- (4) Unless otherwise stipulated above, the liability under this contract corresponds to that of the main contract.

13 Remuneration

The Contractor's remuneration is conclusively regulated in the main contract.

14 Special right of termination

- (1) The Client may terminate the main contract and this Agreement at any time without notice ("extraordinary termination") in the event of a serious breach by the Contractor of data protection regulations or the provisions of this Agreement, if the Contractor is unable or unwilling to carry out a lawful instruction from the Client or if the Contractor refuses to comply with the Client's rights of control in breach of contract.
- (2) A serious breach exists in particular if the Contractor does not or has not fulfilled the obligations specified in this Agreement, in particular the agreed technical and organizational measures, to a significant extent.
- (3) In the event of insignificant violations, the Client shall set the Contractor a reasonable deadline for remedial action. If the remedy is not provided in good time, the client shall be entitled to extraordinary termination as described in this section.

15 Other

- (1) Both parties are obliged to treat all knowledge of business secrets and data security measures of the other party obtained within the scope of the contractual relationship as confidential, even after the termination of the contract. If there is any doubt as to whether information is subject to the confidentiality obligation, it shall be treated as confidential until written release by the other party.
- (2) If the Client's property is jeopardized by third-party measures (such as seizure or confiscation), by insolvency or composition proceedings or by other events, the Contractor must inform the Client immediately.
- (3) The client recognizes this agreement as part of the GTC <https://planubo.com/de/agb/> for the product booked by him.
- (4) The agreement shall commence upon conclusion by the client. If commissioned processing takes place after the end of this agreement, the provisions of this agreement shall apply until the actual end of processing.
- (5) The Contractor may amend the contract at its own discretion with reasonable notice. In particular, the Contractor expressly reserves the right to amend this contract unilaterally if significant legal changes arise in relation to this contract. The Contractor shall inform the Client separately of the significance of the planned amendment and shall also grant the Client a reasonable period of time to declare an objection. The Contractor shall inform the Client in the notification of change that the change shall take effect if the Client does not object within the set period. In the event of an objection by the Client, the Contractor shall have an extraordinary right of termination.
- (6) The exclusive place of jurisdiction for all disputes arising from and in connection with this contract shall be the Contractor's registered office, provided the parties are merchants. This shall apply subject to an exclusive statutory place of jurisdiction. This contract is subject to the statutory provisions of the Federal Republic of Germany and the provisions of European law such as the GDPR.
- (7) Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

Annex 1 - Technical and organizational measures

The order-related technical and organizational measures to ensure data protection and data security, which the contractor must at least set up and maintain on an ongoing basis, are set out below. The aim is to guarantee in particular the confidentiality, integrity and availability of the information processed in the order.

- Encryption (Art. 32 para. 1 lit. a GDPR)
 - Sensitive data, databases and media files that are uploaded are encrypted
 - Confidentiality (Art. 32 para. 1 lit. b GDPR)
 - Access control: No unauthorized access to data processing systems.
 - The Contractor's server and database are located in Germany at Strato AG
 - Images, invoices and uploads are stored on Amazon AWS S3 buckets in Frankfurt
 - Access control: No unauthorized system use
 - Determining the need for protection
 - Implementation of secure access procedures and strong authentication
 - Implementation of simple authentication via user name and password
 - Secure (encrypted) transmission of authentication secrets
 - Blocking in the event of failed attempts and procedure for resetting blocked access IDs
 - Designation of authorized persons
 - Management of personal authentication media and access authorizations
 - Implementation of access restrictions
 - Manual access blocking
 - Access control: No unauthorized reading, copying, modification or removal within the system
 - Assignment of minimum authorizations
 - Client separation: Separate processing of data collected for different purposes
 - Data minimization when handling personal data
 - Regular monitoring of intended use and deletion
 - Separation of test and development environment
 - Integrity (Art. 32 para. 1 lit. b GDPR)
 - Transmission control: No unauthorized reading, copying, modification or removal during electronic transmission or transport
 - Determination of the persons authorized to receive/transmit data
 - Verification of the legality of the transfer abroad
 - Secure data transfer between server and client
 - Secure transmission to external systems
 - Secure storage of data, including backups
 - Data protection-compliant deletion and destruction process
 - Input control: Determining whether and by whom personal data has been entered, changed or removed from data processing systems
 - Logging the entries
 - Availability and resilience (Art. 32 para. 1 lit. b GDPR)
 - Monitoring
 - Resource planning and provision
 - Defense against abuse of the system
 - Data backup concepts and implementation
-

- Recoverability (Art. 32 para. 1 lit. c GDPR)
 - Data backup concepts and implementation
- Data protection organization
 - Definition of responsibilities
 - Implementation and control of suitable processes
 - Obligation of confidentiality
 - Regulations on the internal distribution of tasks
- Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)
 - Process for incident response management
 - Detection and investigation of security incidents
 - Privacy-friendly default settings: If data is not required to achieve the purpose of use, the technical default settings are defined in such a way that data is only collected, processed, passed on or published on the basis of an action by the data subject.
- Order control
 - Selection of further contractors according to suitable guarantees

Annex 2 - Agreement on commissioned processing - Approved subcontractors / other processors

Status: December 20, 2024

Subcontractor	Category	Brief description of the service	Location of the company	Location data	Information on suitable guarantees
Automattic Inc.	Hosting	Website hosting	USA	EU/USA	Certified under the EU-U.S. Data Privacy Framework (adequacy decision)
Amazon Web Services, Inc.	Hosting	Storage of images, invoices and uploads	USA	EU (IE)	Certified under the EU-U.S. Data Privacy Framework (adequacy decision)
Stripe Payments Europe, Ltd.	Payments	Payment processing	EU (IE)	EU/USA	For data transfers to Stripe, Inc., the adequacy decision applies due to the certification under the EU-U.S. Data Privacy Framework
Paddle	Payments	Payment processing and license management	UK	Global	Appropriateness decision
Strato AG	Hosting	Website and data hosting	EN	EN	Not required
Sumo Group Inc (SendFox)	e-mail	E-mail marketing	USA	USA	Standard contractual clauses
Google LLC	Calendar	Scheduling and time planning	USA	Global	Certified under EU-U.S. Data Privacy Framework

					(adequacy decision)
Crisp IM SAS	Communication	Customer chat	FR	EU	Not required
Zoom Video Communications, Inc.	Communication	Video conferencing	USA	EU/USA	Certified under the EU-U.S. Data Privacy Framework (adequacy decision)
Sendinblue GmbH (Brevo)	e-mail	E-mail dispatch	EN	EU	Not required